XXII. Factoring Using Shor's Quantum Algorithm

Quantum Computation, by David P. DiVincenzo, *Physical_and_Theoretical_Chemistry*, Dr. Frank Rioux

This tutorial presents a toy calculation dealing with the quantum factorization of 15 using Shor's algorithm. The first step is to find the period of $\mathbf{a^x}$ **modulo 15**, where **a** is chosen randomly.

$$a := 4 \qquad N := 15 \qquad f(x) := mod\left(a^x, N\right) \qquad Q := 4 \qquad x := 0 .. Q-1 \qquad x = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} \qquad f(x) = \begin{pmatrix} 1 \\ 4 \\ 1 \\ 4 \end{pmatrix}$$

We proceed by ignoring the fact that we can see by inspection that the period of f(x) is 2 and demonstrate how it is determined using a quantum (discrete) Fourier transform. After the registers are loaded with x and f(x) using a **quantum** computer, they exist in the following **superposition**.

$$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|f(x)\rangle = \frac{1}{2}\left[|0\rangle|1\rangle + |1\rangle|4\rangle + |2\rangle|1\rangle + |3\rangle|4\rangle + \cdots\right]$$

The next step is to find the period of f(x) by performing a quantum Fourier transform (QFT) on the input register **|x>**.

$$Q := 4 \qquad mm := 0 .. Q-1 \qquad n := 0 .. Q-1 \qquad QFT_{mm,n} := \frac{1}{\sqrt{Q}} \cdot exp\left(i \cdot \frac{2 \cdot \pi \cdot mm \cdot n}{Q}\right)$$

$$QFT = \begin{pmatrix} 0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5i & -0.5 & -0.5i \\ 0.5 & -0.5 & 0.5 & -0.5 \\ 0.5 & -0.5i & -0.5 & 0.5i \end{pmatrix}$$

$x = 0 \qquad QFT \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.5 \\ 0.5 \\ 0.5 \\ 0.5 \end{pmatrix}$

$x = 1 \qquad QFT \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.5 \\ 0.5i \\ -0.5 \\ -0.5i \end{pmatrix}$

$x = 2 \qquad QFT \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.5 \\ -0.5 \\ 0.5 \\ -0.5 \end{pmatrix}$

$x = 3 \qquad QFT \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0.5 \\ -0.5i \\ -0.5 \\ 0.5i \end{pmatrix}$

The operation of the QFT on the x-register is expressed algebraically in the middle term below.
Quantum interference in this term yields the result on the right which **shows a period of 2 on the x-register.**

$$QFT(x)\frac{1}{2}\left[|0\rangle|1\rangle + |1\rangle|4\rangle + |2\rangle|1\rangle + |3\rangle|4\rangle\right] = \begin{aligned} &\frac{1}{4}\left[|0\rangle + |1\rangle + |2\rangle + |3\rangle\right]|1\rangle \\ &+\frac{1}{4}\left[|0\rangle + i|1\rangle - |2\rangle - i|3\rangle\right]|4\rangle \\ &+\frac{1}{4}\left[|0\rangle - |1\rangle + |2\rangle - |3\rangle\right]|1\rangle \\ &+\frac{1}{4}\left[|0\rangle - i|1\rangle - |2\rangle + i|3\rangle\right]|4\rangle \end{aligned} = \frac{1}{2}\left[|0\rangle\left(|1\rangle + |4\rangle\right) + |2\rangle\left(|1\rangle - |4\rangle\right)\right]$$

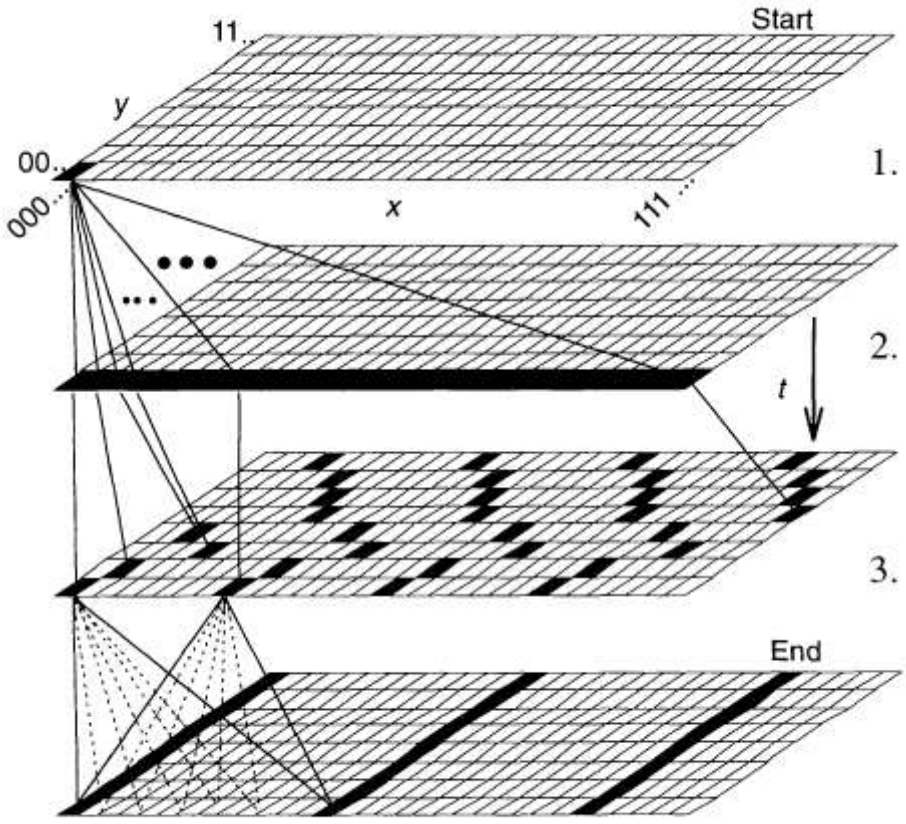
The next step is to use the Euclidian algorithm by calculating the greatest common divisor of two functions involving the period and **a**, and the number to be factored, **N**. This yields the prime factors of 15.

$$period := 2 \qquad gcd\left(a^{\frac{period}{2}} - 1, N\right) = 3 \qquad gcd\left(a^{\frac{period}{2}} + 1, N\right) = 5$$

Figure 5 (Shown Below) in "*Quantum Computation*," by David P. DiVincenzo, *Science* **270**, 258 (1995) provides a succinct graphical illustration of the steps of Shor's factorization algorithm.

> A schematic depiction of the time evolution pathways in Shor's prime factoring procedure. The computational states appearing in the wave function at each selected instant in time are indicated by the filled rectangles. A few of the pathways are sketched out. Most of the pathways in the final step (dotted lines) interfere destructively, with only a few (solid lines) interfering constructively.

The shading in the Figure indicates the instantaneous state vector throughout the three main stages of Shor's computation.



1. Load the x-register:
All zeros. In step 1, the computation is split up into 2^{1000} pathways, so that the wave function of the system becomes a linear superposition of all possible states, with equal phases, of the input register x.

2. Calculate f(x) requiring a single evaluation of a classical Boolean function: **f(x)** = $c^x \pmod N$.
where N is the number to be factored, x is the value of the input register, c is any integer with no prime factors of N. The value of this function is placed in the output register y.

3. Find the period of f(x)
Shor noted that a quantum computer is very well adapted to finding the periodicity of f(x), by means of the execution of a Fourier transform on the input register x.

The Fourier transform takes a wave function of the form, $\Psi_i \rightarrow$

$$\Psi_i = \sum_{x = 00\ldots0}^{11\ldots1} c_x |x\rangle$$

and evolves it in time so that it ends up as Ψ_f or in words, the final wave function coefficients are the discrete Fourier transform of their initial values. Shor observed that this ransformation is a unitary operation and showed that it could be performed in a number of steps polynomial in k, the number of bits in the input register (which is in turn of order the number of bits needed to represent N, the number to be factored).

$$\Psi_f = \sum_{x = 00\ldots0}^{11\ldots1} \left(2^{-k/2} \sum_{x' = 00\ldots0}^{11\ldots1} e^{2\pi i x x'/2^{kl}} c_{x'} \right) |x\rangle$$

$$QFT_{mm,n} := \frac{1}{\sqrt{Q}} \cdot exp\left(i \cdot \frac{2 \cdot \pi \cdot mm \cdot n}{Q}\right)$$